Giovedì, 7 settembre 2000

Presiede:

Guido DE VITA
(Ordinario di diritto della Navigazione nell'Università "Federico II" di Napoli)

GUIDO DE VITA
(Ordinario di Diritto della Navigazione nell'Università "Federico II" di Napoli)

Diamo inizio a questa terza sessione del Convegno – organizzato dal CUST sotto la guida efficiente ed illuminata del professore Fanara, nel quadro delle attività didattiche del Dottorato di ricerca in Diritto della Navigazione e dei Trasporti – riguardante la telematica e le imprese di trasporto. Invito pertanto, il primo dei relatori, il dottore Pagnanelli, Vice Direttore Generale delle Assicurazioni Generali, a prendere la parola.

RELAZIONI

BENITO PAGNANELLI
(Chief Executive of Generali Global – London)

NUOVE TECNOLOGIE E RICERCA NEI TRASPORTI: PROFILI ASSICURATIVI

Premessa.

Signore e signori, buongiorno. Qualcuno di voi mi conosce già perché ho avuto una precedente occasione di parlare in uno dei vostri incontri, sul tema del trasporto aereo e sue implicazioni giuridiche e assicurative. Devo dire che su quel tema mi sentivo un po' più tranquillo perché, partendo dalla Convenzione di Varsavia del 1929, emendata successivamente, si è arrivati oggi a maggiori certezze d'interpretazione, anche se per quanto riguarda i limiti della responsabilità del vettore, tante volte discussi, non si è ancora raggiunta la necessaria uniformità, nelle singole fattispecie di sinistro, sul regime che vuole tale responsabilità illimitata.

Faccio questa premessa perché l'assicuratore oggi, di fronte *all'e-commerce*, si confronta con rischi in parte completamente nuovi e che richiederanno regolamentazioni internazionali che diano certezze. Sono rischi che per l'assicuratore sono gli stessi, sia che riguardino imprese di trasporto, sia che riguardino altre facenti parte del gruppo sempre più numeroso che utilizza le nuove tecnologie di comunicazione.

Vorrei fare un'altra osservazione, o meglio forse una divagazione, in tema di trasporto. Si parla di sviluppo di nuove tecnologie nel trasporto, ma proprio ieri sul "Corriere della Sera" si leggeva della fine, per lo stop ai voli del Concorde, del sogno che un giorno si possano avere mezzi di trasporto che viaggino a 3.000 km. orari.

Qui, direi che l'unica innovazione tecnologica potrà essere costituita in futuro dall'utilizzo delle navette spaziali. Avrete sentito che ci sono società russe e giapponesi che stanno pensando di creare una stazione spaziale dove si farà del turismo, con la costruzione di alberghi, il che genererà ulteriori problemi, non solo di tipo tecnologico, ma anche di tipo medico e giuridico. Se ne dovrà parlare presto.

Tornando al tema, bisogna ricordare che l'assicurazione segue il cambiamento e ad esso deve adeguarsi. Quando il cambiamento significa aumento di valori, l'assicurazione deve essere in grado di coprire questi valori, quando i sistemi giuridici si evolvono l'assicuratore non deve far altro che prendere atto di questa evoluzione e adeguarsi. L'assicuratore non può essere mai promotore del cambiamento ma, piuttosto, deve adeguarsi e, al massimo, consigliare gli attori del cambiamento.

Le nuove tecnologie di cui parliamo devono essere intese come nuovi mezzi di comunicazione e nuovi modi di concludere affari. Noi assicuratori dobbiamo esaminare come si muove il mondo della tecnologia perché è chiaro che gli operatori ci chiedono già soluzioni alle loro esigenze di garanzia.

Non sempre, però, siamo in grado di rispondere, in questa fase ci sono varie teorie sul rischio dell'e-commerce e scarse sono le esperienze. L'assicuratore teorizza anch'esso e, per certi aspetti, considera i rischi dell'*e-commerce* non diversi dai normali danni materiali ai beni: se l'hardware ha un guasto diamo una copertura per i guasti, se il software avesse dei problemi abbiamo la copertura per rischi elettronica, tutte coperture ben consolidate nel tempo.

Si può avere l'interruzione di servizio. Qui dobbiamo dire che l'interruzione nel campo di internet crea dei problemi incredibili a livello di dimensione del rischio da coprire. Abbiamo visto cosa significa un "virus" che gira per il mondo, come quello partito recentemente dalle Filippine. Non è che un virus vada a colpire un solo assicurato, ma tanti, e può creare così dei danni incalcolabili. Da qui derivano le perplessità degli assicuratori di coprire questi rischi secondo metodi e formule tradizionali, che

sono quelli adottati nel campo della *business interruption* più nota. Poi, ci sono i rischi di responsabilità civile che hanno aspetti diversi a seconda del paese in cui si opera.

Per la brevità di questo mio intervento, vi leggo soltanto un elenco stilato da parte di esperti americani di quelli che sono i maggiori rischi di responsabilità civile e certe coperture assicurative connesse, al fine di dimostrare che nell'uso dell'internet e dell'*e-commerce* dobbiamo spesso uscire dai nostri concetti tradizionali: responsabilità per l'utilizzo dei brevetti, per la tutela del marchio, le licenze; la tutela della privacy, il corretto pagamento delle imposte, le attività considerate illegali in certi paesi, la certezza della firma elettronica, le incertezze sul foro competente, sulla giurisdizione, le responsabilità contrattuali da interpretare con il diritto dei vari paesi, la protezione della proprietà intellettuale, e così via.

Non vado avanti perché tante ipotesi di responsabilità potrebbero scoraggiare gli operatori ad utilizzare questi mezzi. Ma credo che sia giusto dare un'illustrazione delle difficoltà che l'utilizzo di queste nuove tecnologie può porre.

In Italia il processo di sviluppo dell'*e-commerce* viene attentamente seguito dal mercato assicurativo che si appresta ad estendere la gamma di coperture fin qui prestate. Oggi, non siamo ancora in grado di dire che questi tipi di rischi trovano una perfetta copertura, ma è una situazione analoga a quella di altri paesi. È chiaro che, se si vuole accelerare una perfetta corrispondenza alle esigenze di copertura, ci deve essere un rapporto di estrema fiducia fra assicuratore e assicurato: davanti a innovazioni di questo genere è doveroso che l'esperienza e i timori siano condivisi.

Ritengo che queste problematiche, qui soltanto accennate, meritino l'attenzione degli studiosi e degli operatori. Sono temi estremamente difficili, ma il commercio e l'attività industriale vanno avanti e anche noi assicuratori dobbiamo adeguarci per fornire il servizio rischiesto.

A questo punto, in appendice, troverete una descrizione più sistematica e, direi, per quanto possibile dottrinaria, delle tipolo-

gie principali di rischio e le ipotesi di copertura, con riferimento anche alle applicazioni nel campo dei trasporti.

Il commercio elettronico e le sue applicazioni.

Ormai da tempo sono diffuse diverse forme di transazione commerciale condotte per vie elettroniche, non solo nell'ambito delle così dette reti "chiuse", cioè con un numero elevato di operatori, ma anche in complesse reti "aperte" su scala globale come internet. Oggi la capillare diffusione di tale potentissimo strumento di comunicazione sta infatti rivoluzionando a livello mondiale il modo di effettuare transazioni commerciali, stravolgendo completamente il modo di organizzare e di strutturare le imprese e cambiando profondamente le relazioni esistenti tra le varie parti coinvolte.

Il Commercio Elettronico può svilupparsi sotto varie tipologie. Convenzionalmente il relativo mercato viene distinto in due categorie:

- *Business to Business:* Nella categoria B-to-B rientrano quelle transazioni che coinvolgono due o più aziende. Un'impresa potrebbe così utilizzare la rete per inoltrare ordini ai propri fornitori, acquisire documentazione, ricevere pagamenti o effettuarne. Nel campo del trasporto di merci si possono localizzare con esattezza i beni trasportati tra la partenza e l'arrivo, con l'utilizzo di un documento elettronico di trasporto in luogo delle tradizionale documentazione di accompagnamento.
- *Business to Consumer:* la categoria B-to-C riguarda le modalità di vendita al dettaglio. Un'azienda offre i propri prodotti a un consumatore finale. Un esempio è dato dalla vendita dei biglietti aerei a mezzo internet. Questa forma di *e-commerce* si è sviluppata con la capillare diffusione di internet negli uffici, nelle case, nelle scuole.

Se, da un lato, questo nuovo *media* consente ad aziende di entrare in contatto diretto con consumatori altrimenti difficilmente

raggiungibili, dall'altro, per i consumatori stessi, si è aperta la possibilità d'avere accesso ad un'offerta amplissima di prodotti.

Per quanto poi concerne le modalità di spedizione del bene al destinatario finale è utile fare una distinzione:

si parla, infatti, di *Commercio Elettronico Indiretto* quando il prodotto è un bene fisico e quindi viene ordinato su Web e spedito tramite corriere;

si parla invece di *Commercio Elettronico Diretto* quando il bene è in forma digitale (ad esempio un software, un documento, un'informazione di borsa) e può essere direttamente trasmesso al cliente via Internet.

Si comprende bene, quindi, come lo sviluppo del commercio elettronico, con la sua fortissima carica innovativa, abbia portato indubbi vantaggi per i suoi utenti. È tuttavia anche corretto dire che l'*e-commerce* ha fatto anche sorgere numerosi problemi di carattere organizzativo e legale completamente nuovi rispetto al passato e che tali problemi hanno generato alcune incertezze che si sta cercando gradualmente di colmare. Si pensi, ad esempio, agli sforzi normativi compiuti da molti Stati per introdurre la firma elettronica o al difficile percorso che ha portato all'adeguamento dei documenti elettronici di trasporto alla normativa ed agli accordi internazionali in materia di trasporto aereo, marittimo e terrestre.

Anche il mercato assicurativo, come già detto, attraverso un'analisi dei nuovi rischi, si sta adeguando a questa realtà.

Mercato assicurativo e nuovi rischi.

Con lo sviluppo dell'*e-commerce* il mercato assicurativo mondiale si è trovato di fronte alla necessità di elaborare, in tempi molto stretti, nuove coperture assicurative atte a garantire gli operatori dai rischi connessi a questa nuova forma di *business*. La strada percorsa è senza dubbio stata quella di avvalersi dei modelli già esistenti per altre tipologie di rischio, con opportune modifiche, sì da cucire una sorta di "polizza su misura".

Alcuni Stati hanno già da tempo fatto propria l'esigenza di provvedere, senza indugio, ad un approfondito esame di questo fenomeno emergente al fine di procedere ad un'opportuna regolamentazione. Tale legislazione ha riguardato soprattutto i c.d. *Trust Service Providers,* ossia quelle organizzazioni preposte alla custodia e tutela di certificati e di firme elettroniche. Sono nati così i primi obblighi di legge inerenti la copertura *Error & Omissions* per la RC derivante da quest'attività di custodia.

Tuttavia, se è ben vero che alcuni paesi stanno allungando il passo in quest'opera di regolamentazione del commercio in rete, in gran parte del mondo – purtroppo – tale processo si sta sviluppando con ben altra velocità e gli operatori (nel nostro caso, gli assicuratori) si trovano costretti a rifarsi ai più rodati princìpi di legge regolanti il commercio tradizionale.

Ovviamente, come succede del resto nell'assicurazione dei rischi per così dire "tipici", per usare un termine di tipo privatistico, non tutto è assicurabile come avviene ad esempio nella copertura del c.d. "rischio imprenditoriale" nella RC professionale. È chiaro come ci siano dei limiti a quello che si può assicurare: l'assicuratore non può essere chiamato a rispondere per le conseguenze economiche derivanti da scarse capacità imprenditoriali!

Volendo quindi procedere ad una sintetica panoramica su queste nuove coperture vediamo come, anche nel caso dell'*e-commerce*, esistano garanzie assimilabili a quelle tradizionali, quali quelle *property, business interruption, loss of revenue, professional liability*. Troviamo poi altre fattispecie che, seppur traendo spunto da formule tradizionali, più si attagliano al settore informatico come, ad esempio, la garanzia per i rischi da *computer crime*.

Va chiaramente ammesso che, in tutto questo settore, forti sono le influenze delle esperienze fatte dagli Stati Uniti, che da tempo hanno data particolare impulso a questo settore. Le schematizzazioni che seguono si basano infatti su molti princìpi e regole di quel paese.

1. *Infringement.*

Gli operatori di *e-commerce* sono senza dubbio esposti ogni giorno a varie fattispecie d'*infringement*. La differenza sostanziale rispetto alle consuete forme di commercio sta nell'amplificazione del problema data dalla facilità d'accesso ad internet ed alla possibilità di operare anonimamente.

1.*1* *Copyright Infringement.*

È questa la forma più comune di *infringement*. Negli Stati Uniti, ad esempio, la legge federale sul *copyright* protegge il lavoro originale dell'autore definito in un ben individuato mezzo di espressione. Tale disciplina stabilisce una responsabilità assoluta per la violazione di cinque diversi tipi di *copyright*: *reproduction*, *distribution*, *modification*, *public performance* e *public display*.

1.*2* *Patent Infringement.*

Negli Stati Uniti, i brevetti sono disciplinati da una legge federale: il *Patent Act*. Ai diversi Stati è quindi proibito garantire protezione simile a quella già fornita dal *Patent Act*. Detta legge federale protegge le invenzioni riguardanti procedimenti, apparecchiature, manufatti, *compositions of matter* (anche noti come *utility patents*, ossia brevetti d'invenzioni che rappresentano un progresso tecnico nel settore specifico) e *ornamental design* (*design patent*, brevetti del *design*). Le invenzioni protette da *utility patents* possono essere elettriche, meccaniche, chimiche o di natura biologica. La concessione di *utility* o *design patents* è soggetta a rigorosi requisiti.

Numerosi brevetti sono stati concessi in relazione a tecnologie internet, a procedimenti, a *design* e perfino a metodi computerizzati per lo svolgimento di attività commerciali. Con la diffusione di internet, è facile poter sviluppare in maniera indipendente una tecnologia o un procedimento simile ad uno già protetto da brevetto.

Coperture assicurative disponibili

Per quanto riguarda il *patent infringement*, le coperture assicurative disponibili sul mercato sono:

- *General Liability*: la violazione del brevetto (*patent infringment*) non può verificarsi nel corso di attività pubblicitarie poiché un brevetto può essere violato solo producendo, usando o vendendo un articolo brevettato. Poiché la copertura fornita per la violazione (*infringement*) è in relazione alla sola fattispecie dell'*Advertising Injury*, non viene fornita alcuna copertura per la mera contraffazione del brevetto.
- *Media Professional Liability:* questo tipo di copertura include spesso la copertura *Defensive Patent Infringment* per specifici brevetti.
- *Intellectual Property Coverage*: un numero limitato di polizze c.d. *Defensive and Offensive (Enforcement) Coverage* sono disponibili su particolari mercati e per specifici tipi di brevetti.

1.*3* Trademark Infringement/Cybersquatting.

Trademarks

I marchi di fabbrica (*trademarks*) ed i marchi di servizi (*service marks*) sono rappresentati da parole, nomi, simboli o insegne utilizzati dai produttori e dai fornitori di servizi per identificare le loro merci ed i servizi e per distinguerli dalle merci prodotte e dai servizi forniti da altri. Sempre negli Stati Uniti, per i marchi usati in commercio, la protezione del marchio di fabbrica è regolata da una legge federale, il *Lanham Act*.

Come detto sopra, la protezione del marchio di fabbrica è disponibile per parole, nomi, simboli o insegne in grado di distinguere le merci o i servizi di un soggetto da quelli di altri. Un marchio di fabbrica che descrivesse semplicemente una classe di merci piuttosto che distinguere il marchio di un produttore rispetto alle merci fornite da altri, non potrebbe trovare analogo riconoscimento giuridico.

Domain Names

La tutela dei diritti sui *domain names* e sul *trademark* può in parte coincidere. Anche laddove un nome associato ad una società non sia stato da questa registrato, esso può comunque essere definito un *trademark* per il fatto stesso di essere stato associato a questa determinata società. Ciò ha dato luogo a numerose vertenze sulla proprietà e sull'utilizzo dei *domain names*.

Negli Stati Uniti, il *Federal Trademark Dilution Act* conferisce titolo ad agire per la c.d. *trademark dilution,* ossia per l'utilizzo non autorizzato del marchio che tende ad indebolire, offuscare o ossidare il valore commerciale di marchi famosi. Tale legge federale viene utilizzata dai titolari di un *trademark* al fine di impedire a terzi l'utilizzo del proprio marchio come *domain name* su internet.

Una pratica meglio nota come *cybersquatting* è andata diffondendosi nel caso di indirizzi internet, particolarmente interessanti, registrati (*domain addresses*) senza alcuna intenzione di utilizzarli, ma semplicemente per poterli poi rivendere a scopo di profitto. Vediamo, infatti, come si sia spesso verificato il caso di registrazione di un indirizzo da parte di un individuo utilizzando un nome comune quale, ad esempio, *www. macdonalds.com* e del successivo tentativo da parte di tale individuo di vendere l'indirizzo all'organizzazione con marchio simile. Le grandi società commerciali hanno tentato di contrastare questa pratica rivendicando la protezione del *trademark* del *domain address*. Sempre negli Stati Uniti, nel 1998, la Corte d'Appello del nono Circuito ha stabilito che il *cybersquatting* costituisce violazione del *Trademark Dilution Act.*

Il 5 agosto 1999, il Senato degli Stati Uniti ha approvato la proposta di un *Anti Cybersquatting Consumer Protection Act* (S. 1255) con lo scopo di limitare il fenomeno del *cybersquatting*. Questo progetto di legge consentirebbe ai titolari di *trademark* di ottenere *statutory damages* in quei casi in cui venisse provato che un *trademark* sia stato registrato in mala fede da una persona

con il solo scopo di ricavarne, slealmente, un profitto dalla vendita del c.d. *trademarked name*. Tale provvedimento permetterebbe inoltre ai titolari di *trademark* di rivendicare il loro diritto in *rem* chiedendo la confisca, la cancellazione o il trasferimento di un *domain name* in violazione dopo aver dimostrato al giudice adito di aver tentato, senza risultati, di localizzare la persona che aveva registrato il *domain name*.

L'Ufficio *Patent and Trademark* americano ha riportato un considerevole aumento delle richieste di registrazione di *domain names* come *trademark*. Tale registrazione fornisce un efficace punto di partenza per

- evitare che, negli Stati Uniti, altri possano ottenere *domain names* identici.
- impedire la registrazione di *trademark* simili che potrebbero dar luogo a confusione.

Oltre ai più noti problemi legati all'utilizzo dei *trademark*, Internet presenta alcune singolari possibilità di violazione del *trademark*.

Metatags

Poiché le parole contenute nei *web sites* verranno trovate dai motori di ricerca ed usate per identificare quel determinato sito, i progettisti dei *web sites* tentano di massimizzare l'uso dei *trademark* per attirare l'attenzione dei motori di ricerca.

I *metatags* sono parole contenute in codici non visibili sul *web site* ma che possono essere individuate dai motori di ricerca. Inserire *trademarks* di proprietà altrui in questo codice può costituire una violazione del *trademark* e/o configurare l'ipotesi di concorrenza sleale. Tuttavia, i tribunali hanno riconosciuto la legittimità di alcuni utilizzi dei *metatags*. I tribunali non hanno riscontrato infatti alcuna violazione del *trademark* qualora questo venga usato, in buona fede, per inserire nell'indice il contenuto del *web site*.

Links

L'abilità nell'usare i *trademarks* negli *hyperlinks* può senz'altro ingenerare confusione negli utenti di internet. Nel caso *Playboy Enterprises, Inc. vs. Universal Tel-A-Talk, Inc.*, il convenuto fu ritenuto responsabile dell'utilizzo del marchio di *Playboy* sia in un *hyperlink* sia in una *navigational bar* della sua *home page*. Tali *link* promuovevano invece prodotti in concorrenza con quelli di *Playboy*. Tale utilizzo dei *links* ingenerava alla fine confusione nel consumatore che poteva erroneamente ritenere che link identificassero i prodotti dell'attore (*Playboy*). In questo caso, l'utilizzo di *links* o *framed links* può dare origine alla pubblicità dei prodotti del convenuto in luogo di quelli della parte attrice con ciò causando una perdita di profitto e di pubblicità.

Anche se alcuni aspetti del *linking* sono stati messi in discussione, talvolta l'utilizzo di *trademark* altrui insieme con il *linking* può essere considerato legittimo.

File and Directory Names: molte azioni legali sono state intraprese in relazione all'utilizzo dei *trademark* nei *file* o *directory names*.

Territorial Boundaries: tradizionalmente, la legge sui *trademark* garantisce al titolare del *trademark* il diritto esclusivo di utilizzare il marchio in un'area geografica ben definita. Ora, poiché la pubblicazione di una pagina web equivale alla pubblicazione a livello nazionale, anzi, a livello mondiale, la violazione di un *trademark* sul quale il titolare ha un diritto di esclusiva in un paese può comportare la contemporanea violazione di diritti di altre persone in altre giurisdizioni. In effetti, i tribunali hanno riscontrato violazione in alcuni casi sulla base dell'uso di un marchio su un *web site*. Trattandosi di una nuova area legislativa non è ancora ben chiaro come, in definitiva, i giudici e le corti tratteranno questo conflitto intrinseco.

Coperture assicurative disponibili.

Le coperture assicurative disponibili sul mercato sono:

- *General Liability:* la tipica polizza di R.C. Generale non fornirà copertura alle rischieste di risarcimento del danno causato da violazione del *trademark* o del *servicemark*. Il modello ISO 1998 fornirà copertura alle richieste di risarcimento da violazione di *Trade Dress* nel settore della pubblicità. I modelli 1993 e 1998 garantiranno la copertura dei danni da violazione del titolo e dello stile nella condotta degli affari nel campo pubblicitario che possono permettersi una certo livello di copertura. Tuttavia, nel caso *Lebas Fashion Imports of USA vs. ITT Hartford Insurance Group*, un tribunale californiano ha ritenuto che la clausola *advertising injury* nella polizza fosse ambigua e che quindi la violazione del *non-advertising trademark* fosse coperta.
- *Multi-Media Policies*: tali polizze eliminano il requisito del nesso pubblicitario tipico di una polizza di R.C. Generale e spesso includono la violazione del *trademark*, il plagio o l'utilizzo non autorizzato di titoli, formati, idee, personaggi, trame, rappresentazioni artistiche, o altro materiale descrittivo, invasione di privacy, diffamazione scritta, verbale ed altre forme di diffamazione.
- *E-Commerce Policies:* le varie polizze supplementari *E-Commerce* forniscono copertura per i costi di difesa inerenti richieste di danno derivanti da violazione del *trademark* o del *servicemark*, ma devono essere utilizzati testi di polizza *ad hoc* al fine di determinare l'estensione della copertura prestata. Poche polizze forniscono altresì una difesa adeguata nei confronti di azioni legali che mirano a provvedimenti esecutivi tesi al ripristino della situazione *quo ante*.

1.*4 Inevitable Misappropriation doctrine.*

La c.d. *Inevitable Misappropriation Doctrine* risale a più di trenta anni fa. Gli ex datori di lavoro che ricorrono ai giudici per richiedere provvedimenti di natura ingiuntiva nei confronti degli ex dipendenti che cominciano un nuovo lavoro con un concorrente si avvalgono, in genere, di tale dottrina per proteggere i propri segreti industriali. I requisiti

per ottenere questo tipo di provvedimenti ingiuntivi sulla base della dottrina sopra richiamata sono riassunti in un test diviso in tre sezioni, nel quale test l'ex datore di lavoro deve provare ai giudici che:

a) l'ex dipendente è a conoscenza dei segreti industriali del primo datore di lavoro (test della conoscenza);

b) le mansioni del nuovo lavoro del dipendente (ed i prodotti e la tecnologia sui quali lavora) sono talmente simili o collegati a quelli che svolgeva nella precedente posizione che sarebbe per lui estremamente difficile non fare affidamento su di esse o non utilizzare i segreti industriali del primo datore di lavoro (test della affinità di impiego); e

c) non si può fare affidamento sull'ex dipendente e sul nuovo datore di lavoro – per un certo numero di ragioni che vanno dall'ignoranza, negligenza fino alla mala fede – affinché non utilizzino le informazioni sul segreto industriale (test di lealtà).

1.5 *Other Infringements/violations.*

Le attività commerciali su internet sono altresì esposte all'accusa di violazioni a diverso titolo tra cui la contraffazione o violazione di:

- *Trade Secrets*
- *Trade Dress*
- *Title*
- *Mask Works*
- Informazioni Confidenziali
- *Non Disclosure Agreements*
- *Licenses*
- *Franchises*

Coperture assicurative disponibili.

Le coperture assicurative disponibili sul mercato sono:

- *General Liability:* la polizza di R.C. Generale fornisce copertura alla *"pubblicazione scritta o verbale di materiale che viola il diritto alla* privacy *di una persona"*. Il modello ISO 1998 garantisce la copertura dei danni causati dalle violazioni di *Trade Dress* durante la promozione pubblicitaria di merci, di servizi o prodotti. Il furto di segreti industriali non è coperto perché la violazione avviene come conseguenza del furto e non nel corso di un'attività pubblicitaria. Un'eccezione a questa regola è stata fatta dai giudici in quei casi in cui il furto include liste di clienti e tecniche di marketing utilizzate per sollecitare tali clienti ad acquistare prodotti o servizi di concorrenza.
- *Multi-Media Policies:* queste polizze eliminano il requisito del nesso pubblicitario tipico di una polizza di R.C. Generale e spesso includono la violazione del *trademark*, il plagio e l'utilizzo non autorizzato di titoli, formati, idee, personaggi, trame, rappresentazioni artistiche, o altro materiale descrittivo, invasione della *privacy*, diffamazione scritta, verbale o altre forme di diffamazione.
- *E-Commerce Policies*: le varie polizze supplementari E-Commerce forniscono copertura per i costi di difesa inerenti richieste di danno derivanti da violazione del *trademark* o del *servicemark,* ma devono essere utilizzati testi di polizza *ad hoc* al fine di determinare l'estensione della copertura prestata. Poche polizze forniscono altresì una difesa adeguata nei confronti di azioni legali che mirano a provvedimenti esecutivi tesi al ripristino della situazione *quo ante.*

2. *Defamation.*

Il termine *diffamazione* si usa per descrivere sia la diffamazione scritta che quella verbale. La diffamazione rappresenta la perdita di reputazione di un individuo, come la diffamazione commerciale o discredito (denigrazione) di un prodotto rappresenta una perdita per il prodotto stesso o per l'attività commerciale. La giurisprudenza costante dei tribunali americani vuole che i venditori ed i distributori di pub-

blicazioni diffamatorie siano ritenuti responsabili solo qualora venisse dimostrata l'effettiva consapevolezza, da parte loro, di una condotta diffamatoria. Tale condizione *sine qua non* trova il suo fondamento nelle costituzionali garanzie di libertà di parola e di stampa di cui al Primo Emendamento.

In particolare, il *Communications Decency Act* del 1996 esonera i *service providers* di internet (ISP) da responsabilità per diffamazione nel caso in cui dimostrino l'esistenza di procedure interne di *screening* volte ad evitare la pubblicazione di materiale diffamatorio. Tuttavia, questa garanzia non viene estesa alla maggior parte di quei datori di lavoro i cui dipendenti utilizzino e-mail ed internet.

A questo riguardo anche il patrocinio o lo svolgimento di un servizio di *chat* o di *bulletin board* pone importanti (e tuttora non ancora risolte) questioni di responsabilità conseguenti alla citata disciplina sulla diffamazione. Poiché il solo scopo dei servizi di *chat* e di *bulletin board* è quello di consentire agli utenti di inviare messaggi e di dialogare, detti utenti potrebbero compiere atti diffamatori o violare diritti di *copyright* inviando messaggi o scaricando materiale *on line*. Alcune decisioni prese da tribunali americani in ordine alla determinazione se l'operatore di un servizio di *chat* o di un *bulletin board* sia in effetti un mero distributore oppure un editore vero e proprio evidenziano come la discriminante sia da individuarsi nel livello di controllo redazionale esercitato dall'operatore.

Inoltre, è importante determinare se la diffamazione commessa in una *chat room* debba essere considerata diffamazione scritta oppure orale in quanto alcune giurisdizioni richiedono la prova dell'effettivo danno sofferto al fine di configurare la diffamazione orale, ma non per quella scritta.

Coperture assicurative disponibili.

Le coperture assicurative disponibili sul mercato sono:

- *General Liability:* la sezione *Personal Injury* di una tipica polizza di R.C. Generale potrà fornire copertura ai danni da diffamazione di persone, merci o servizi derivanti da pubblicazione scritta od orale di materiale utilizzato nello svolgimento di un'attività di *e-commerce*.
- *Multi-Media Policies*: tali polizze eliminano il requisito del nesso pubblicitario tipico di una polizza di R.C. Generale e spesso estendono la garanzia alla violazione della *privacy*, alla diffamazione scritta od orale e ad altre forme di diffamazione.

3. *Privacy.*

Le tradizionali questioni di protezione della *privacy* si applicano anche alle attività commerciali svolte a mezzo internet ed – ovviamente – sono amplificate dalla facilità con cui gli operatori di *e-commerce* sono in grado di raccogliere e catalogare informazioni personali e confidenziali.

Infatti, la preoccupazione per la sicurezza dei dati personali è la ragione principale addotta dai consumatori per non effettuare acquisti su internet. Tale timore è inoltre giustificato anche dalla prassi per alcuni siti internet di vendere le informazioni sui propri clienti. Esempi di informazioni personali sui clienti spesso catalogate nei database degli operatori a cui si può accedere via internet sono:

- informazioni sul credito
- precedenti finanziari
- storia personale / preferenze
- passwords
- precedenti penali
- informazioni mediche

All'inizio del 1998 il FTC effettuò una verifica su oltre 1400 siti industriali per determinare il grado di protezione della *privacy* dei clienti. Tale audit rivelò che, mentre l'85% dei siti presi a campione raccoglievano informazioni personali dei consumatori, soltanto il 14% di questi rendevano note le pratiche di raccolta dei dati e solo il 2% rendeva disponibile la propria politica sulla privacy dei clienti. Su queste basi, il FTC concludeva che gli sforzi dell'industria per incoraggiare l'adozione volontaria delle più elementari pratiche di informazione non erano adeguati alle esigenze di tutela dei consumatori. A seguito di questo rapporto del FTC per il Congresso e del timore che il governo federale potesse imporre una propria disciplina di regolamentazione, i vari gruppi industriali si sono attivati al fine di incentivare l'autoregolamentazione.

Negli Stati Uniti, sulla base *dell'Electronic Communications Privacy Act del 1986*, la posta elettronica (e-mail interpersonali) gode delle medesime garanzie di protezione riservate alla posta di prima classe. Tuttavia, fanno eccezione a questa disciplina gli e-mail degli impiegati che possono essere controllati dal datore di lavoro. A questo riguardo ricordiamo peraltro come, in un recente caso, un tribunale del Minnesota abbia riconosciuto il datore di lavoro responsabile di violazione della *privacy* del dipendente a causa di intercettazione di messaggi elettronici.

Coperture assicurative disponibili.

- *General Liability:* una tipica polizza di R.C. Generale potrà fornire copertura soltanto ai danni derivanti dalla pubblicazione scritta o verbale di materiale utilizzato nell'espletamento di un'attività di e-commerce. Sarebbero quindi esclusi dalla copertura i danni da *breach of security* aventi come immediata conseguenza una violazione della *privacy* del cliente (quando, ad esempio, a causa di limitati livelli di sicurezza un *hacker* riesce a penetrare le *fire walls* e ad impadronirsi di informazioni confidenziali).
- *Multi-Media Policies:* tali polizze eliminano il requisito del nesso pubblicitario tipico di una polizza di R.C. Generale e spes-

so estendono la garanzia alla violazione della privacy, alla diffamazione scritta od orale e ad altre forme di diffamazione.

- *E&O:* molti clausolari *E&O* prevedono l'esclusione della *Breach of security* e, di conseguenza, limitano la possibile copertura della violazione della *privacy*.

4. *Legal & Regulatory issues.*

4.*1 Taxation.*

Anche se gli operatori di *e-commerce* sostengono l'inapplicabilità di imposte statali e locali sulle vendite elettroniche qualora la società operatrice non abbia una sede nello stato in cui le vendite vengono effettuate mediante il sito web, i 30.000 diversi enti federali, statali o locali preposti alle tasse presenti negli Stati Uniti sono ben consapevoli del potenziale reddito derivante dal commercio elettronico su internet. Ciascuno di questi enti potrebbero, potenzialmente, imporre una tassa sulle quote mensili di abbonamento a Internet, sulla vendita di merci e servizi e su ogni singolo *bite* di informazione digitale trasmesso via internet. Ad oggi, ben otto Stati hanno prodotto leggi tendenti alla tassazione dell'accesso o del commercio su internet. Il potenziale per una tassazione molteplice e differenziale sulle transazioni effettuate su internet è naturalmente ovvio.

Con in mente questa confusione sulla potenziale tassazione, alla fine del 1998, il Congresso degli Stati Uniti ha approvato l'*Internet Tax Freedom Act* (ITFA), divenuto poi parte integrante dell'*Omnibus Consolidated Appropriations Bill* del 1998. Il Presidente Clinton ha firmato l'*Appropriation Bill*, incluso l'IFTA, il 21 ottobre 1998. L'Atto prevede quattro disposizioni fondamentali, la più importante delle quali è data dalla previsione che, a partire dall'1 ottobre 1998, viene imposta una moratoria di tre anni sulle tasse d'accesso ad internet ed una tassazione molteplice o discriminatoria sul commercio elettronico.

È stato quindi costituito dal Congresso degli Stati Uniti un *Internet Tax Panel* presieduto da David Pottruck della *Charles Schwab* con lo scopo di delineare un'opportuna politica di tassazione per le transazioni effettuate a mezzo internet. In qualità di sottocomitato dell'*Advisory Committee on Electronic Commerce*, questo gruppo di esperti ha quindi predisposto un ordine del giorno che prevede la possibilità per i Governi locali di tassare le merci vendute su Internet o su catalogo o di tassare il mero accesso a internet.

La *National Governors' Association* si è pubblicamente opposta alla politica di non tassazione adottata dalla Casa Bianca, anche se corre l'obbligo di segnalare come alcuni governatori siano sostenitori di un mercato su internet esente da tasse.

4.*2* ***Regulated Products.***

Non è chiaro il modo in cui la pubblicità ed i criteri di vendita per prodotti regolamentati come farmaci, bevande alcoliche ed armi verranno fatti rispettare. Il 10 giugno 1999 il Presidente Clinton ha emesso un ordine esecutivo che poneva il Procuratore Generale Janet Reno a capo di un gruppo incaricato di redigere un rapporto il cui scopo era di determinare se le leggi esistenti fossero sufficienti a indagare e perseguire crimini su internet quali la vendita di armi, esplosivi, sostanze controllate e farmaci su prescrizione come pure la frode e la pornografia infantile.

Per fare un esempio, *Amazon.com* e *Barnesandnoble.com* sono stati informati dal Governo tedesco che la vendita da parte loro di libri anti semitici come *Mein Kampf* in Germania costituisce una violazione della legge tedesca. Da ciò deriva che qualunque attività commerciale a mezzo internet deve essere effettuata con una certa cautela al fine di garantire la conformità con leggi e discipline amministrative in vigore in ciascun paese in cui vengono venduti e/o pubblicizzati i prodotti.

- Farmaci: di norma, negli Stati Uniti, la FDA deve approvare tutte le pubblicità e tutte le etichette. La FDA non ha peraltro indicato ad oggi se intenda essere altrettanto rigorosa nel richiedere ai siti web di pubblicare *disclaimer* su ogni singola pagina o, in alternativa, fornire l'intero contenuto del sito per approvazione.

Considerando tuttavia che le pagine web possono essere talvolta modificate anche giornalmente, non è chiaro come le richieste della FDA possano essere interamente rispettate, in pratica, dagli operatori di internet. Finora la FDA non ha chiarito a sufficienza la propria posizione, anche se si è impegnata a studiare e sviluppare una coerente politica applicabile ai siti web.

- Bevande alcoliche: il 20 luglio 1999 l'*House Judiciary Committee* ha approvato un progetto di legge destinato a conferire agli Stati dell'Unione l'autorità di perseguire le società che violano le leggi in vigore nel medesimo stato in relazione alla vendita di alcolici. Sulla base di questo progetto, gli Stati potrebbero quindi portare dinanzi alla Corte Federale società residenti al di fuori dello stato stesso. La proposta darebbe inoltre agli Stati maggior potere in relazione alla riscossione delle tasse sugli alcolici venduti a mezzo internet nel proprio territorio. Ciò, presumibilmente, non violerebbe la moratoria sulle nuove tasse su internet in quanto si focalizza sulla riscossione di tasse già esistenti. Tuttavia, se questo progetto venisse trasformato in legge vera e propria, si porrebbe immediatamente la questione della riscossione delle tasse sulle vendite effettuate a mezzo internet.
- Armi: una proposta volta ad includere nel citato progetto di legge anche la vendita di armi su internet è stata subito scartata e nessun provvedimento alternativo è stato preso in merito a questo problema.

4.3 *Freedom to Speech.*

Nel caso *Reno vs. the ACLU*, la Corte Suprema ha stabilito che il Primo Emendamento si applicava anche ad internet e ha

quindi cassato alcune delle previsioni contenute nel *Communications Decency Act*. La corte del Nono Circuito ha decretato in *Bernstein vs. US Department of Justice* che il *computer source code* (ma non gli *object code*) merita completa protezione sulla base del Primo Emendamento. Il *source code* è di solito scritto in linguaggi come il BASIC e può essere letto da una persona piuttosto che soltanto dal computer. Tale decisione è stata peraltro oggetto di ricorso da parte del Departrment of Justice e potrebbe arrivare fino alla Corte Suprema a causa di questioni di sicurezza nazionale riguardanti la distribuzione di tecnologia *encryption.*

4.*4 Sec Regulations.*

Il *Securities Act* del 1933, nella sua versione emendata, prescrive che l'offerta e la vendita di titoli vengano effettuate in conformità ad una dichiarazione di registrazione/iscrizione depositata presso la *Securities and Exchange Commission (SEC)*, salvo che non venga altrimenti disposto. Inoltre, anche nel caso in cui i titoli siano stati validamente registrati con la SEC, la Sezione 10 del *Securities Act* del 1933 dispone che qualunque materiale scritto riguardante un'offerta debba adeguarsi al prospetto registrato.

La SEC ha fatto causa a promotori e società per offerte e vendite illegali a mezzo internet. D'altro canto, alcune società sono riuscite ad effettuare con successo offerte limitate ai sensi della *Rule 504* della *Regulation D*, che disciplina le offerte inferiori a 1 milione di dollari, e/o della *Regulation A*, che regola le offerte con un prezzo totale inferiore a 5 milioni di dollari. Molto è stato scritto in merito agli aumenti di capitale a mezzo internet. Una piccola fabbrica di birra, chiamata *Spring Street Brewing*, con sede a New York, è stata la prima società a vendere pubblicamente le proprie azioni su internet sulla base della *Regulation A* e a raccogliere 1.6 milioni di dollari con un'offerta diretta utilizzando un prospetto *on-line* per stimolare gli investitori.

Da allora un certo numero di offerte pubbliche è stato effettuato per mezzo di internet.

Le società che vogliono utilizzare internet per offerte *offshore* di titoli, lo possono fare, se l'offerta viene effettuata in conformità con la *Regulation S* della SEC. La SEC ha infatti predisposto procedure e speciali requisiti per tali offerte. Se una società tenta di aggirare questa disciplina approfittando di una *private placement exemption* al fine di evitare la registrazione federale e statale previste per un'offerta di titoli, deve ricordare che qualunque riferimento all'offerta fatta sul proprio sito internet può essere considerata pubblicità vietata od offerta al pubblico. L'esonero di cui alla *Regulation D* del *Securities Act* del 1933 vieta la pubblicità e l'offerta pubblica come condizione *sine qua non* per l'applicazione dell'esonero. Per questa ragione la società non deve in alcun caso fare riferimento ad un'eventuale offerta privata di titoli sul proprio sito.

Nel caso di un'offerta convenzionale di titoli, le informazioni rese pubbliche sul sito web della società devono inoltre essere riesaminate onde evitare situazioni di incompatibilità con eventuali dichiarazioni contenute in un prospetto o memorandum di offerta privata. I siti web tendono inoltre ad essere particolarmente orientati verso il marketing, in completo contrasto con le tipiche dichiarazioni precauzionali incluse nei documenti informativi dei *securities disclosure documents*. I legali della società dovrebbero altresì premurarsi affinché le informazioni pubblicate sul sito non possano essere ritenute una forma di pubblicità vietata dell'offerta al fine di evitare la cancellazione o ritardi dell'offerta.

Attualmente la SEC e la maggior parte delle parallele organizzazioni a livello statale sembrano disposte a consentire alle società l'uso di internet per "sondare il terreno" al fine di verificare l'esistenza di un mercato per l'offerta di titoli (in conformità con la *Rule 254* della SEC). Tuttavia, le società emittenti non possono effettuare alcuna vendita senza prima aver inoltrato una dichiarazione di emissione alla SEC.

Per le *public companies*, anche le informazioni sul sito web dovrebbero essere vagliate per assicurare la coerenza con le registrazioni depositate presso la SEC e con le dichiarazioni fatte in ossequio ad obblighi di legge o di organismi di controllo (quali ad esem-

pio gli organismi di contro e disciplina delle banche e delle compagnie di assicurazione).

4.5 *Illegal activities.*

Gli operatori di siti web devono prestare la massima attenzione a non violare le leggi esistenti nei vari paesi. Il problema in effetti è legato al fatto che internet non conosce confini e, pertanto, un'attività, che può essere considerata legale in una giurisdizione, potrebbe non esserlo in un'altra.

Per esempio, sempre negli Stati Uniti, il gioco d'azzardo *on-line* è legale in alcuni Stati ma espressamente vietato in altri (Illinois, Louisiana, Nevada e Texas). In questo caso anche se un sito *on-line* per il gioco d'azzardo tenta di verificare lo stato di residenza dei suoi giocatori d'azzardo, qualora un giocatore residente in uno stato in cui il gioco d'azzardo *on-line* sia proibito riesca egualmente ad accedere al sito, potremmo trovarci in una situazione di violazione di legge. In effetti, il Dipartimento di Giustizia ha fatto causa a 22 siti internet per il gioco d'azzardo sulla base del *Wire Communications Act*. Detto atto vieta ai giocatori di azzardo di usare un mezzo di comunicazione via cavo per la trasmissione, nel commercio interstatale o con l'estero, di scommesse su qualsiasi evento o contesto sportivo. Questa legge era stata emanata originariamente per agevolare i Governi statali nella repressione del crimine organizzato collegato alle scommesse. Qualora organizzazioni straniere (quali, ad esempio, i casinò) offrano gioco d'azzardo ai cittadini locali in violazione delle leggi locali, gli Stati potranno probabilmente assistenza a livello federale. A questo proposito il Senato degli Stati Uniti sta valutando l'opportunità di utilizzare l'*Internet Gambling Prohibition Act* del 1999 per impedire l'uso di internet per il gioco d'azzardo o per la trasmissione di informazioni utili per l'impresa del gioco d'azzardo.

Per fare un altro esempio, in un recente caso radicato in Alabama e Wisconsin, alcune maggiori compagnie di carte di credito sono state citate in giudizio per aver violato le leggi statali e federali a causa della riscossione di debiti contratti in seguito a gioco d'azzardo illegale a

mezzo internet. Ancora, le case d'aste *on-line* spesso inseriscono fotografie degli oggetti d'arte offerti per la vendita. Mentre questa pratica è considerata un uso corretto di opere coperte da *copyright* negli Stati Uniti, è invece considerata illegale in Francia.

Le etichette delle confezioni di vitamine e dei prodotti alimentari conformi agli standard statunitensi potrebbero non esserlo per la legge di altri paesi. Ciò è particolarmente vero quando si tratta di prodotti alimentari contenenti sostanze modificate geneticamente: mentre tale situazione è piuttosto comune negli Stati Uniti, è invece proibita nella maggior parte dei paesi dell'Unione Europea.

La legge inglese sulla diffamazione è senz'altro più severa di quella statunitense e non garantisce gran parte delle difese per diffamazione riconosciute negli Stati Uniti.

4.*6 Spam & Netiquette.*

L'uso della posta elettronica ha reso possibile raggiungere milioni di potenziali consumatori semplicemente premendo un tasto e ad un costo praticamente nullo per colui che opera sul mercato.

L'utilizzo indiscriminato degli e-mail, tuttavia, può esasperare e infastidire la maggior parte dei destinatari di questi *"e-mail* spazzatura*"* (*junk e-mail*).

Negli Stati Uniti, a seguito alla forte avversione da parte degli operatori nel settore internet per questo tipo di corrispondenza non richiesta, sono già stati avanzati, sia a livello federale che statale, disegni di legge destinati a regolamentare l'uso della posta elettronica. Alcune leggi statali vietano messaggi e-mail non richiesti a meno che non siano immediatamente identificabili come pubblicità e che contengano il nome di chi li invia, l'indirizzo e l'indirizzo e-mail. Altre estendono la portata di leggi statali già esistenti sui "fax spazzatura" (*junk fax*) per includere gli e-mail non richiesti mentre altre ancora prescrivono che gli autori di e-mail istituiscano un numero verde (toll-free) che permetta al ricevente di chiamare e scegliere di non ricevere più corrispondenza in futuro.

Nel caso *1267623 Ontario Inc. us. Nexx Online Inc.*, la Corte Superiore di Giustizia dell'Ontario ha stabilito, in data 14 giugno 1999, che – sulla base dell'esame dei princìpi emergenti dalla giurisprudenza delle corti americane, dagli estratti delle documentazioni fornite e dalle reazioni dei singoli utenti di internet –, a meno che il *service provider* non preveda, *ab initio*, nel contratto la diffusione non richiesta di una notevole quantità di materiale pubblicitario via e-mail, risulta chiaro che l'invio via e-mail di tale materiale non richiesto a scopi pubblicitari è contrario ai principi della *Netiquette.*

La cosiddetta *Netiquette*, anche se nella maggior parte dei casi non scritta, sta diventando rapidamente la legge (*common law*) che regola le transazioni su internet.

4.7 *Digital signature & Certificates.*

La firma digitale non è altro che un modo di firmare un documento elettronico e di assicurarne la sua fondamentale integrità. L'uso di certificati e firme digitali si rende necessario al fine di garantire la correttezza delle transazioni su internet.

Al fine di rendere possibile la verifica dell'autenticità di una firma digitale, la firma elettronica contiene spesso un certificato digitale emesso da una "autorità di certificazione" (*CA*). Una CA è di fatto assimilabile ad un notaio elettronico che verifica l'identità della persona che chiede la certificazione.

È possibile ripartire in due distinti gruppi gli Stati che consentono l'uso delle firme digitali (quelli che autorizzano le firme digitali sia per comunicazioni pubbliche che private e quelli che autorizzano tali firme soltanto per uso pubblico):

- Arizona, California, Idaho, Indiana, Maryland, Mississippi, New Mexico, North Carolina, North Dakota, Rhode Island e Texas autorizzano l'uso delle firme elettroniche per la corrispondenza elettronica con i Dipartimenti di Stato e le agenzie pubbliche;

- Alaska, Florida, Georgia, Illinois, Kansas, Kentucky, Minnesota, Mississippi, Nebraska, New Hampshire, Oklahoma, Oregon, South Carolina, Utah, Virginia, Washington, West Virginia e Wisconsin autorizzano l'uso delle firme digitali sia per rapporti pubblici che per quelli privati.

A livello internazionale, le norme riguardanti le licenze di una CA sono piuttosto varie e spesso oscure. La bozza della *Directive on Electronic Signatures* dell'Unione Europea vieta agli Stati membri di richiedere una concessione per le CA, ma consente una sorta di concessione volontaria. A livello mondiale esistono diverse iniziative in campo legislativo riguardanti le firme digitali. Se tali regolamentazioni dovessero pervenire a risultati molto diversi, potrebbero compromettere l'uso delle firme elettroniche nel commercio internazionale.

La responsabilità della CA nei confronti del destinatario del messaggio in relazione a inesattezze o false dichiarazioni contenute nel certificato è, a tutt'oggi, poco chiara.

4.*8* *Privacy Legislation & Regulations.*

Anche se il Governo federale degli Stati Uniti protegge l'accesso ai propri database, non esiste di fatto alcuna disciplina per i database privati contenenti dati personali.

Più di 40 paesi hanno emanato o intendono emanare leggi sulla privacy che tutelino l'uso dei dati personali dei consumatori. Il Parlamento Europeo ha promulgato nel 1995 una direttiva entrata in vigore il 26 ottobre 1998. L'articolo 26 di tale direttiva vieta a qualunque società che svolge attività commerciali nell'Unione Europea di trasmettere dati personali ad un paese che non garantisce analoga tutela della *privacy*. Il *Commerce Department* degli Stati Uniti ha quindi predisposto un proprio rapporto in risposta alla direttiva della U.E. Con tale rapporto si evidenzia come il ruolo del Governo federale sia quello di consigliare, fare pressioni e patrocinare, ma non quello di intervenire a livello legislativo, fatta eccezione per alcuni settori come quelli dei *medical records* e la *privacy* del bambino.

Nella gran parte dei casi, la *FTC* e l'Amministrazione Clinton sono state più propense ad incentivare l'autoregolamentazione. In proposito, il Presidente della FTC Robert Pitofsky ha già sostenuto come l'autoregolamentazione, se utilizzata in modo corretto, potrebbe offrire una flessibilità che la legislazione e la burocrazia non avranno mai. Tuttavia, Pitofsky ha anticipato l'eventualità di un intervento diretto da parte del Congresso qualora l'autoregolamentazione da parte dei privati non dovesse dimostrarsi sufficientemente adeguata.

L'attenzione dell'Amministrazione Clinton sulle questioni relative alla *privacy* si è poi concretizzata, nel marzo 1999, nella nomina del Prof. Peter Swire dell'Università Statale dell'Ohio a primo *Chief Counselor* del paese in materia di *privacy*. Secondo il programma, almeno inizialmente, Swire dovrebbe concentrarsi sulla soluzione dei conflitti emersi fra Stati Uniti e Unione Europea a seguito dell'entrata in vigore della citata severa direttiva dell'Unione Europea sulla *privacy*. Infatti, sulla base di detta direttiva, le società statunitensi potrebbero trovarsi nell'impossibilità di utilizzare informazioni su consumatori europei.

Per evitare che gli operatori statunitensi possano subire un taglio nella trasmissione dei dati internazionali da parte della U.E., l'Amministrazione Clinton ha proposto di creare dei "porti" sicuri per consentire alle ditte di continuare ad effettuare lo scambio di dati qualora detti operatori si siano adeguati volontariamente a degli standard fondamentali sulla *privacy*.

Infatti, non più tardi del novembre 1998, l'Amministrazione Clinton ha reso nota una proposta d'adeguamento volontario da parte degli operatori statunitensi per rispondere alle esigenze della direttiva europea. Sulla base di questa proposta, le società che si attengono a "sette princìpi" generali verrebbero considerate in regola con le previsioni della normativa europea. Tali "sette principi" riflettono le intese intercorse fra l'Amministrazione Clinton e gli operatori commerciali ma, di fatto, non sono stati mai approvati dalla U.E. In effetti, i paesi della U.E. ritengono che il

Governo federale degli Stati Uniti non imponga agli operatori una efficace protezione della *privacy*.

Il c.d. *Electronic Communications Privacy Act* (*ECPA*) statunitense disciplina l'accesso non autorizzato e la divulgazione di messaggi di posta elettronica. Il Titolo 18 del *United States Code (USC)* regolamenta l'attività del Governo federale e garantisce ai vari enti federali l'autorità di promulgare leggi e regolamenti volti alla disciplina dell'accesso a documentazioni elettroniche. Un esempio di questi possibili interventi è dato dalla decisione di considerare un'infrazione federale l'accesso ad un *network* di computer senza autorizzazione o eccedere un determinato numero di accessi autorizzati su qualsiasi rete di computer. La ECPA non fornisce tuttavia analoga tutela sul posto di lavoro, principalmente perché la ECPA trova applicazione alla sola "*intercettazione*" di messaggi elettronici e non alla revisione di messaggi memorizzati.

Mentre ai datori di lavoro è vietato monitorare telefonate o trasmissioni via e-mail di un impiegato nelle quali lo stesso impiegato può aspettarsi un ragionevole livello di *privacy*, la ECPA riconosce ai datori di lavoro la possibilità di monitorare trasmissioni elettroniche qualora gli impiegati stessi vengano avvisati in anticipo o se il datore di lavoro abbia ragione di credere che gli interessi della società possano essere compromessi.

Il 17 luglio 1998 il disegno di legge *The Children's Online Privacy Protection Act* veniva presentato dal senatore Bryan del Nevada. Detta proposta veniva quindi trasformata in legge come parte integrante dell'*Omnibus Appropriations Bill.* In sostanza, il progetto di legge richiedeva che la *Federal Trade Commission* emanasse una disciplina tesa a tutelare la riservatezza in merito ad informazioni personali su internet relative ai bambini. In particolare, detta disciplina dovrebbe imporre agli operatori commerciali di siti web l'ottenimento del consenso dei genitori, peraltro facilmente verificabile, per raccogliere ed usare informazioni personali relative ai bambini al di sotto di 13 anni.

4.9 *Jurisdiction.*

Di fatto, internet sottopone gli operatori commerciali al rispetto delle leggi applicabili in molteplici giurisdizioni. In questo scenario plurigiurisdizionale, che potrebbe comportare la prospettiva di regolamenti contrastanti, la possibile esposizione a contenzioso civile costringe detti operatori a valutare in anticipo gli standard legali in base ai quali la loro condotta sarà poi valutata. In questo modo gli Stati possono, di fatto, esercitare la propria giurisdizione su cittadini ed operatori commerciali stranieri qualora detti cittadini od operatori avessero contatti sistematici con detto Stato o fossero ritenuti responsabili di azioni illecite compiute a mezzo internet in tale Stato.

Tuttavia, anche in questo settore, le tendenze possono essere le più varie. Infatti, molti possono essere i criteri per valutare la portata delle operazioni del sito web al momento di determinare la giurisdizione del cittadino straniero. Mentre la maggioranza dei giudici americani sembra essere riluttante a stabilire la propria giurisdizione unicamente sulla base della presenza nel territorio dello Stato di un sito web passivo, altre corti hanno optato in questo senso. Nei casi che coinvolgono siti web interattivi, la giurisdizione viene generalmente determinata esaminando il livello di interattività e la natura commerciale delle informazioni che vengono trasmesse *on-line*.

Vediamo poi come, ad esempio, poiché i consumatori possono accedere via internet ai siti web domiciliati in tutte le possibili giurisdizioni degli Stati Uniti, la creazione di un sito web *on-line* potrebbe potenzialmente comportare questioni di autorizzazioni (licenze, permessi) multigiurisdizionali per i liberi professionisti (medici, contabili, avvocati, agenti assicurativi, ecc.) e questioni legate a pubblicità illegale non richiesta.

Gli aspetti connessi alla giurisdizione continuano ad essere oggetto di accesi dibattiti nelle corti americane. In *Fix My PC, L.L.C., et al. vs. N.F.N. Associates Inc. Et al.*, la corte ha stabilito che la presenza di un sito web "passivo" non fosse sufficiente a determinare la sussistenza della giurisdizione sull'operatore

commerciale. In *PurCo Fleet Services In. vs. Micheal Towers, et al.*, i giudici decidevano invece che l'esistenza di un sito web che permette agli utenti di entrare in contatto via e-mail costituisce una transazione d'affari nello stato dell'Utah.

Aspetti assicurativi.

È evidente che qualsiasi polizza che preveda limitazioni territoriali e non fornisca una garanzia *worldwide* potrebbe esporre l'assicurato a buchi di copertura.

5. *Contractual Liabilities.*

5.*1 Breach of Contract.*

Se le merci o i servizi pubblicizzati sul sito e successivamente venduti non sono poi all'altezza delle aspettative dell'acquirente o utente, la parte venditrice potrebbe essere esposta ad una richiesta di risarcimento per inadempimento contrattuale.

5.*2 Online Contracts.*

Le transazioni contrattuali *on-line* sono spesso effettuate mediante l'uso di contratti *web-wrap*. Un contratto *web-wrap* altro non è che un'offerta trasmessa su internet e la relativa accettazione trasmessa in risposta dal cliente che clicca sul suo computer "accetto". Ora, mentre i contratti *web-wrap* trovano sempre maggiore diffusione, non è ancora chiaro quale possa essere l'effettivo livello di protezione garantito a queste transazioni da parte dei tribunali.

A causa della scarsa giurisprudenza in materia di contratti *web-wrap*, alcuni giuristi si sono rifatti alle sentenze in merito ai c.d. *shrinkwrap* o *clickwrap* nel campo del software. In effetti, in alcuni casi è stata confermata, per analogia, l'applicabilità della disciplina giuridica relativa a tali contratti anche alla vendita di

merci su internet. Poiché la legislazione vigente ed i *case law* in materia non sono al passo con lo sviluppo dell'*e-commerce* e delle sempre più pressanti questioni relative alla formazione di un contratto in un contesto elettronico, la nuova bozza dell'articolo 2B dell'*Uniform Commercial Code (UCC)* potrebbe fungere da modello per futuri regolamenti statali e per eventuali casi giurisprudenziali. L'*American Law Institute* (ALI) ha in effetti predisposto una bozza di legge commerciale uniforme che potrebbe trovare applicazione alle transazioni elettroniche ed alla tutela del software.

In base all'articolo 2B i contratti conclusi a mezzo internet avrebbero, in sostanza, piena validità e sarebbero quindi immediatamente vincolanti e sanzionabili. L'assenza di un contratto scritto potrebbe, in linea teorica, rappresentare un ostacolo al riconoscimento della validità di un contratto *on-line*. Tuttavia, l'UCC 2B cerca di risolvere questo aspetto mediante la sostituzione della parola *"writing"* con *"record"*. Ovviamente, tale modifica terminologica non è meramente semantica, bensì determinante nel deviare l'interpretazione giuridica dai princìpi tradizionali legati al valore della forma scritta e nel conferire valenza giuridica al *record* elettronico in quanto equivalente funzionale della firma apposta su un modulo cartaceo.

L'UCC 2B introduce inoltre il nuovo concetto di *"electronic agent"*. L'introduzione di un "agente elettronico" è decisamente innovativa rispetto alle leggi in vigore in materia di contratti. Essenzialmente, si riconosce la possibilità di stipulare contratti elettronici senza l'intervento dell'uomo. Di conseguenza, un computer può automaticamente effettuare le formalità di offerta e di accettazione, che – fino ieri – non potevano prescindere da una qualche forma di intervento umano.

Sforzi per trovare un accordo sulla versione finale dell'articolo 2B sono stati fatti recentemente sulla scia dell'opposizione da parte di alcuni gruppi industriali nel campo dell'*entertainment* e della comunicazione. Infatti, alcune associazioni, incluse Motion Picture Association of America, National Association of Broadcasters, National Cable Television Association, Recording Industry Association of America, Newspaper Association of America e Magazine Publi-

shers of America hanno insistito affinché l'applicabilità del UCC 2B venga limitata al solo software e non quindi anche alle transazioni elettroniche. Tuttavia, è molto probabile che, alla fine, le varie parti interessate si accorderanno su una versione finale che potrà essere utilizzata come base per le transazioni elettroniche, ivi incluse le transazioni assicurative condotte via internet.

5.3 *Conflicts with other Channels of Distribution.*

Molte società vendono oggi i loro prodotti non solo attraverso i tradizionali canali di distribuzione, ma anche via internet. L'uso di questi due diversi sistemi può creare conflitti inaspettati. Infatti, i contratti di distribuzione tradizionale potrebbero attribuire un diritto di esclusiva nella commercializzazione di un particolare prodotto o servizio in una data area geografica. Ora, poiché i siti web non si rivolgono ad un certo settore geografico, le vendite effettuate via internet potrebbero essere in conflitto con questi accordi di esclusiva.

5.4 *Denial of Service/Repudation of Access.*

Il c.d. *denial of service attack* a computer collegati ad internet provoca l'interruzione del collegamento o il blocco del computer. I *denial of service attacks* sono considerati un reato federale sulla base del *National Information Protection Act* del 1996. Le sanzioni includono considerevoli pene pecuniarie e la detenzione. Gli attacchi al *sistema operativo* hanno come obiettivo i buchi nella sicurezza del sistema. Tali buchi possono tuttavia essere "rappezzati" per prevenire attacchi ripetuti. Le ultime versioni di molti sistemi operativi quali, ad esempio, Windows 98, MacOS 8 e Linux sono già sicuri contro tali attacchi. Gli attacchi ai *network* spesso non possono essere rappezzati e non è possibile prevenirli e difenderci. Tali attacchi possono penetrare il *bandwidth* e causare danni al *network* stesso. Anche se la maggior parte dei titolari di siti web su internet ritengono di non essere responsabili per eventuali perdite eco-

nomiche sofferte da un cliente che non riesce ad accedere al loro sito (o a causa della lentezza dell'accesso dovuti a traffico), in alcuni tribunali sono attualmente pendenti azioni tese a dimostrare che l'operatore del sito web è contrattualmente obbligato a fornire l'accesso. Conseguenza immediata e diretta per il proprietario del sito web, oltre al costo di difesa da tali accuse, è sicuramente dato dalla perdita di clienti e dalla pubblicità negativa che può allontanare dal sito potenziali nuovi clienti.

5.5 *Unauthorized Access.*

L'accesso non autorizzato ad informazioni confidenziali – che comporti o meno una perdita economica per il proprietario dell'informazione – è sicuramente una questione critica per le società che svolgono attività commerciali su internet. Molti operatori di *e-commerce* specificano il tipo di *router*, di *firewall* e le procedure di sicurezza che ciascuno dei suoi partner su internet deve utilizzare per proteggere i propri dati. Alcuni, come ad esempio la Cisco Systems, richiedono ai propri tecnici di valutare le misure di sicurezza di un partner e ritiene detti partner responsabili per qualunque buco nella sicurezza. Ora, mentre questa pratica trova sempre maggiore diffusione, un buco nelle misure di sicurezza comporterà delle responsabilità contrattuali.

6. *Extortion.*

Mentre tutte le attività commerciali in genere possono essere esposte ad estorsioni legate a minacce di danni a persone o cose, il commercio elettronico scopre nuovi scenari alle possibili forme di intimidazione. L'estorsione può concretizzarsi nella minaccia di:

- chiudere la rete mediante un *Denial of Service Attack*

- assumere il controllo da lontano (remotely) di operazioni critiche per mezzo di un "cavallo di Troia"
- svelare informazioni confidenziali o imbarazzanti
- danneggiare o distruggere dati.

7. *Damage to property.*

Tale assicurazione riguarda la copertura di danni a cose, proprietà, macchinari, dati, ecc. Tali danni devono, ovviamente, essere causati da un evento accidentale. Con tale copertura, l'assicuratore garantisce, di norma, la copertura dei costi di rimpiazzo dei beni persi o danneggiati oppure, ad esempio, il costo della ricostruzione delle banche dati andate accidentalmente distrutte.

È sicuramente questo uno dei rischi cui un'azienda moderna e tecnologicamente avanzata è sottoposta quotidianamente. Aziende che fondano la loro attività sul commercio elettronico sono particolarmente vulnerabili alla perdita di profitto derivante da danni a beni o cose, propri o altrui, ma vitali per il *business* dell'azienda.

7.*1* *First Party.*

Tali attività commerciali possono essere esposte ad eventi naturali, alla negligenza di impiegati o *contractors* nonché di eventuali terzi. Che il danno sia stato provocato accidentalmente o dolosamente, l'impatto economico è sempre lo stesso. L'azienda può correre il rischio di veder la propria attività commerciale cessare o soffrire penalizzazioni più o meno gravi in caso di danneggiamento, distruzione o manomissione a:

- computers, reti, server, web sites, intranet, extranet, e-mail;
- software, firmware;
- banche dati elettroniche, *off line libraries;*
- *electronic media*;
- impianti di telecomunicazione;

- satelliti;
- *Service providers* o altri *contractors*

Le coperture assicurative *first party* disponibili sul mercato sono:

- *Property Insurance*: le polizze spesso contengono massimali molto limitati per i danni causati da virus ed espongono gli assicuratori al rimborso dei costi necessari alla ricostruzione delle banche dati o al rimpiazzo del mero supporto elettronico sul quale i dati erano archiviati. Gran parte di queste polizze escludono la disonestà dei dipendenti a meno che non si tratti di atti di vandalismo. Appare evidente tuttavia come, in questo campo, sia molto difficile dare una definizione di atto di vandalismo e non è chiaro se gli atti compiuti dagli *hackers* o la diffusione di virus possano essere considerati atti vandalici.
- *Business Income:* questo tipo di polizze opera in genere solo in presenza di una corrispondente polizza per danni alla proprietà. Ciò comporta che, in assenza di una simile garanzia, la perdita di profitto derivante da danni o furto di proprietà intellettuale non sarebbe coperta.

7.2 *Intellectual Property.*

Dipendenti o esterni possono rubare o copiare *intellectual property* (software, procedure varie, ecc.) vitali per l'operatività del commercio elettronico. La definizione di *"intellectual property"* nell'*e-commerce* è senza dubbio più ampia di quella utilizzata nei settori tradizionali dei brevetti, dei *copyrights*, dei *trade rights* e *R&D*. Nel caso dell'*e-commerce*, la proprietà intellettuale può includere *sound bytes*, codici di programma, stili e formati utilizzati per particolari business, colori, procedure, conoscenze e tecnologie.

Il valore della proprietà può essere talvolta determinato non dai dati bensì dalle procedure utilizzate per la gestione dei dati stessi. È chiaro come sia oltremodo difficile quantificare il valore di questo tipo di informazioni. Tale valutazione non può prescindere e dal va-

lore intrinseco del dato e dalle azioni che possibili concorrenti potrebbero intraprendere qualora dette informazioni venissero rivelate.

Il furto o la copia di proprietà intellettuale può senza dubbio comportare perdite di profitto, di quote (o di potenziali quote) di mercato, di opportunità di business, danni all'immagine, costi di riproduzione dei dati rubati o copiati ecc.

La perdita di dipendenti "chiave" a vantaggio della concorrenza può essere fonte di preoccupazione allorquando detti dipendenti abbiano avuto accesso alla *intellectual property* dell'azienda. Va da sé che, qualora detti impiegati abbiano contribuito alla creazione di questa proprietà intellettuale, hanno essi stessi sviluppato conoscenze tali da poter creare seri danni nel caso di divulgazione a detti concorrenti delle informazioni in loro possesso.

Altra fattispecie può configurarsi nell'impedire l'accesso alla proprietà intellettuale. Tale situazione è meglio nota come *"breach of utility"* e si verifica allorquando il dipendente o terzi criptino documenti importanti impedendo così l'accesso a coloro non in possesso della chiave di decriptazione. Una *"breach of utility"* può essere provocata, intenzionalmente, dal dipendente scontento che lascia l'azienda oppure, in buona fede, dall'impiegato che più semplicemente dimentica la chiave di decriptazione.

Le coperture assicurative *intellectual property* disponibili sul mercato sono:

- *Property Insurance:* le polizze spesso contengono massimali molto limitati per i danni causati da virus ed espongono gli assicuratori al rimborso dei costi necessari alla ricostruzione delle banche dati o al rimpiazzo del mero supporto elettronico sul quale i dati erano archiviati. Tali polizze non rispondono in genere delle conseguenze economiche derivanti dalla perdita di potenzialità di mercato a seguito di furto di proprietà intellettuale.
- *Business Income*: questo tipo di polizze operano in genere solo in presenza di una corrispondente polizza per danni alla proprietà. Ciò comporta che, in assenza di una simile garanzia, la perdita di profitto derivante da danni o furto di proprietà intellettuale non sarebbe coperta.

- *Intellectual Property Coverage*: queste polizze sono di norma limitate alla violazione dei brevetti (*patent infringement*) e forniscono copertura sia alle spese di difesa che a costi di azioni nei confronti di terzi.

8. *Crime Exposure.*

Negli ultimi dieci anni molte attività commerciali sono diventate sempre più computer dipendenti anche se non vengono esercitate via internet. I negozi al dettaglio non possono registrare una vendita quando i computer sono spenti; i fabbricanti non possono rintracciare una merce quando il sistema è *off line*, ecc. Accumulare informazioni critiche e/o procedimenti in un singolo database è come avere un'unica fonte che fornisce un determinato articolo: se il sistema si blocca, non hai alternative.

Con l'inserimento di queste informazioni in un'applicazione accessibile via internet, l'esposizione non è necessariamente aumentata, ma è sicuramente accresciuta la facilità di accesso all'informazione stessa. Alcuni dei possibili rischi collegati alle operazioni di *e-commerce* comprendono:

- perdita di fondi durante un trasferimento (bonifico) elettronico – sia per frode che per errore;
- frode su computer;
- furto, distruzione o modifica di dati o proprietà intellettuale;
- incapacità di verificare o incassare pagamenti/effetti attivi.

Coperture assicurative disponibili.

- *Computer Fraud Coverage*: disponibile sia come allargamento della Fidelity Coverage o da sola;
- *Funds Transfer Fraud Coverage*;
- *Computer Virus Coverage;*
- *Property Coverage;*
- *Fidelity Coverage;*
- *Financial Institutions Bonds.*

9. *Disaster Recovery.*

Per un'attività commerciale elettronica, la perdita del collegamento può avere effetti disastrosi – indipendentemente dalle ragioni o dal lasso di tempo. Basta pensare che l'operatore potrebbe avere una sola possibilità di attirare un potenziale cliente nel suo sito e, in caso di assenza di collegamento, il cliente potrebbe non accedere più al suo sito. I clienti regolari possono essere in qualche modo più indulgenti, ma interruzioni nel collegamento per lungo tempo o ripetute più volte dirotteranno rapidamente l'acquirente via internet sul sito di un concorrente.

Trattandosi di un'industria del tutto nuova, per *l'e-commerce* esistono solamente alcuni *case studies* e nessun *off the shelf disaster recovery plan*. I tradizionali *disaster recovery plan* sono in genere rivolti alla azioni da intraprendere a seguito di catastrofi naturali, incendi ed altri danni alla proprietà. Tali piani, in genere, vengono predisposti per far sì che l'impresa possa ritornare in attività nel più breve tempo possibile. Per molte attività *e-commerce* (per esempio compravendita elettronica e servizi bancari elettronici) un periodo di interruzione anche soltanto di alcune ore sarebbe inaccettabile.

Oltre alle possibili esposizioni tradizionali, un *disaster plan* per *l'e-commerce* dovrebbe prevedere specifiche procedure in relazione a:

Prevenzione.

- sicurezza fisica del sito
- linee guida per il caso di estorsione
- applicazione dei princìpi guida relativi ai diritti sulla proprietà intellettuale
- princìpi guida sull'utilizzo dell'e-mail
- princìpi guida sull'utilizzo di internet
- princìpi guida anti-plagio
- documentazione sulla proprietà intellettuale e valutazioni
- istruzione dei dipendenti per la prevenzione dei disastri e per la ripresa

Planning.

- revisioni periodiche del programma per la ripresa della centrale dati
- *contingent power* e *utility supply*
- duplicazione di *business processes* e dati
- notifica al cliente e procedure di comunicazione
- cosa fare nel caso di un attacco per minimizzare il danno e la durata dell'interruzione
- processi forensi
- *hot-site*, *warm-site* o *cold-site switch over plans*
- spazio ed equipaggiamento alternativo per lo staff
- accesso alternativo ad internet
- metodi per fornire supporto tradizionale al cliente durante i periodi di crisi
- sicurezza per proprietà intellettuale e dati confidenziali durante i periodi di crisi
- *crisis management of brand image*
- controllo/gestione delle informazioni ai media

10. *Consumer Fraud.*

I notiziari sono pieni di storie su consumatori che sono stati imbrogliati su internet – merci mai consegnate, aste fraudolente, frodi sulle carte di credito, ecc. Tecnologie come gli *escrow services online* ed i "portafogli sicuri" vengono utilizzati assieme ai certificati digitali per rendere le transazioni più sicure.

Le società che forniscono merci e servizi via internet possono a loro volta essere defraudate dai consumatori stessi. Le perdite causate da vendite fraudolente raggiungono oggi circa l'un per cento del reddito *on-line.* La *Federal Trade Commission,* la *SEC* e diversi *attorney generals* stanno studiando a fondo i meccanismi della frode via internet.

11. *Antitrust/Unfair Competition.*

Violazione delle leggi sulla pubblicità, pratiche ingannevoli e concorrenza sleale comprendono diversi modi impropri di svolgere attività commerciali, comprese l'azione o pratica commerciale illecita, sleale o fraudolenta e la pubblicità sleale, ingannevole, falsa o fuorviante. Le società si rendono responsabili di simili condotte allorquando pubblicano informazioni false, fuorvianti e non verificate riguardanti le proprie attività commerciali sul web.

La pratica ingannevole comprende la falsa indicazione di origine e/o sponsorizzazione su un web site e la pubblicità falsa.

Un tipo di pratica fuorviante ampiamente utilizzato in internet è quella di trarre vantaggio da un errore di digitazione del consumatore. Per esempio, fino al 23 luglio 1999 un consumatore che sillabava erroneamente www.geico.com con www.geigo.com sarebbe finito in un sito chiamato *AllStates Car Insurance*. Anche se un *disclaimer* affermava che il sito non era collegato alla *Allstate Insurance Co.*, gli utenti che cliccavano per ottenere una quotazione venivano mandati al sito web di *Progressive Insurance Company*. Questo sito è stato chiuso dopo le lamentele di Geico.

12. *False advertising.*

Le richieste di danni per falsa pubblicità sono spesso effettuate sulla base della sezione 43(a): del *Federal Lanham Act* che stabilisce che "Chiunque, in rapporto con determinate merci o servizi ... utilizzi nel commercio qualunque ... descrizione di fatti falsa o fuorviante, o rappresentazione dei fatti falsa o fuorviante, la quale ... in pubblicità o promozione, rappresenti erroneamente la natura, le caratteristiche, le qualità, o l'origine geografica delle sue o altrui merci, servizi, o attività commerciali, verrà ritenuto responsabile in un'azione civile da chiunque ritenga di essere o di poter essere danneggiato da un atto di questo tipo".

Per promuovere una richiesta di danni per pubblicità falsa, una società deve provare le cinque cose:

- una falsa dichiarazione di fatto del convenuto in una pubblicità commerciale su un suo o altrui prodotto;
- la dichiarazione ha effettivamente ingannato o tende ad ingannare un considerevole segmento del suo pubblico;
- l'inganno è materiale nel senso che probabilmente influenzerà la decisione di acquistare o meno;
- il convenuto ha provocato la diffusione della sua falsa dichiarazione nel commercio tra stati: e
- il querelante è stato leso o sarà probabilmente leso a causa di questa falsa dichiarazione, sia attraverso una deviazione diretta delle vendite da lui al convenuto, sia dalla diminuzione del valore dell'avviamento associato ai suoi prodotti.

I consumatori non possono fare causa per falsa pubblicità secondo il *Federal Lanham Act*. Infatti, lo scopo dell'*Act* è quello di "tutelare le persone impegnate ... nel commercio contro la concorrenza sleale" e non di tutelare i consumatori. Le leggi statali forniscono comunque ai consumatori rimedi nei casi di errata rappresentazione.

13. *Tortius interference.*

Una società può citare in giudizio il proprietario di un sito web se quest'ultimo ha ingiustamente interferito con suoi rapporti commerciali e, di conseguenza, provocato un danno economico.

L'attore può fare causa per il danno ingiustamente sofferto laddove non esistano rapporti contrattuali, come pure nel caso in cui l'interferenza non sia intenzionale.

GUIDO DE VITA
(c.s.)

Ringrazio il dottore Pagnanelli per le tante cose interessantissime che ha avuto la cortesia di dirci. Ci ha delineato, infatti, sinteticamente, ma con estrema chiarezza, i ruoli dell'assicurato e dell'assicuratore, delimitando il campo di azione del primo e definendo la collaborazione che a volte l'assicuratore ritiene di dovere chiedere all'assicurato. Ci ha pure manifestato qualche perplessità sull'attuale stato dell'evoluzione del mondo assicurativo. E' ben noto che l'assicurazione è figlia della scommessa, però credo che oggi, pur se una "scienza non esatta" - come l'ha definita il dottore Pagnanelli - l'assicurazione debba, comunque, essere considerata una scienza, la quale si va perfezionando giorno per giorno. Naturalmente, perfezionarsi in una fase in cui, come in quella attuale, vi è una continua evoluzione tecnologica non è semplice. Il dottore Pagnanelli ha sottolineato pure il ruolo e i rischi dell'amministratore di fatto al momento dell'apposizione delle firme in via meccanica. L'amministratore che travalica i suoi poteri è per noi una realtà di tutti i giorni, però in campo assicurativo, per le cose che ha sottolineato il dottor Pagnanelli, il problema assume una delicatezza enorme.

Invito, adesso, il dottor Cirillo Orlandi, Amministratore delegato della SINPORT, a svolgere la sua relazione su "Nuove tecnologie e organizzazione delle imprese di trasporto".